UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,994	08/31/2001	Takuya Morishita	Q66052	9297

7590 04/24/2006

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/942,994	MORISHITA, TAKUYA	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 26, 2006 has been entered.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 18 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 18 is directed to a method for decrypting an encrypted computer program where this process is an abstraction and does not provide physical transformation of the plurality of blocks of the computer program. The specification discusses the blocks but the blocks are not defined. Thus, is directed to an abstract idea where claim 18 is a "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component.

According to the MPEP,

The subject matter courts have found to be outside the four statutory categories of invention is limited to abstract ideas, laws of nature and natural phenomena. While this is easily stated, determining whether an applicant is seeking to patent an abstract idea, a law of nature or a natural phenomenon has proven to be challenging. These three exclusions recognize that subject matter that is not a practical application or use of an idea, a law of nature or a natural phenomenon is not patentable. See, e.g., Rubber-Tip Pencil Co. v. Howard, 87 U.S. (20 Wall.) 498, 507 (1874) ("idea of itself is not patentable, but a new device by which it may be made practically useful is"); Mackay Radio & Telegraph Co. v. Radio Corp. of America, 306 U.S. 86, 94, 40 USPQ 199, 202 (1939) ("While a scientific truth, or the mathematical expression of it, is not patentable invention, a novel and useful structure created with the aid of knowledge of

scientific truth may be."); Warmerdam, 33 F.3d at 1360, 31 USPQ2d at 1759 ("steps of locating' a medial axis, and creating' a bubble hierarchy . . . describe nothing more than the manipulation of basic mathematical constructs, the paradigmatic abstract idea'"). Courts have expressed a concern over "preemption" of ideas, laws of nature or natural phenomena. The concern over preemption was expressed as early as 1852. See Le Roy v. Tatham, 55 U.S. 156, 175 (1852) ("A principle, in the abstract, is a fundamental truth; an original cause; a motive; these cannot be patented, as no one can claim in either of them an exclusive right."); Funk Brothers Seed Co. v. Kalo Inoculant Co., 333 U.S. 127, 132, 76 USPQ 280, 282 (1948) (combination of six species of bacteria held to be nonstatutory subject matter). The concern over preemption serves to bolster and justify the prohibition against the patenting of such subject matter. In fact, such concerns are only relevant to claiming a scientific truth or principle. Thus, a claim to an "abstract idea" is nonstatutory because it does not represent a practical application of the idea, not because it would preempt the idea.

Nonstatutory Subject Matter
Claims to computer-related inventions that are clearly nonstatutory fall into the same general categories as nonstatutory claims in other arts, namely natural phenomena such as magnetism, and abstract ideas or laws of nature which constitute "descriptive material." Abstract ideas, Warmerdam, 33 F.3d at 1360, 31 USPQ2d at 1759, or the mere manipulation of abstract ideas, Schrader, 22 F.3d at 292-93, 30 USPQ2d at 1457-58, are not patentable. Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support
specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data.

If the "acts" of a claimed process manipulate only numbers, abstract concepts or ideas, or signals representing any of the foregoing, the acts are not being applied to appropriate subject matter. Schrader, 22 F.3d at 294-95, 30 USPQ2d at 1458-59. Thus, a process consisting solely of mathematical operations, i.e., converting one set of numbers into another set of numbers, does not manipulate appropriate subject matter and thus cannot constitute a statutory process.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4, 6-9, 11-14, and 16-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Rix, et al. (US 6,766,024).

As per claim 1:

Rix discloses a system for decrypting an encrypted computer program, comprising:

means for generating a first cipher key from at least one first block of the encrypted computer program; **(col.2, lines 36-37 and col.3, lines 17-18)**

means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key; **(col.2, lines 44-45)**

means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. **(col.1, lines 35-39 and col.2, lines 46-50)**

As per claim 2: **See col.2, lines 7-8;** discussing wherein said at least one a first block is not encrypted.

As per claim 3: **See col.2, lines 36-37 and col.3, lines 17-18;** discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 4: **See col.2, lines 38-39;** discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 6:

Rix discloses a method for decrypting an encrypted computer program, comprising the steps of:

generating a first cipher key from at least one first block of the encrypted computer program; **(col.2, lines 36-37 and col.3, lines 17-18)**

performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key; **(col.2, lines 44-45)**

means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. **(col.1, lines 35-39 and col.2, lines 46-50)**

As per claim 7: **See col.2, lines 7-8;** discussing said at least one first block is not encrypted.

As per claim 8: **See col.2, lines 36-37 and col.3, lines 17-18;** discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 9: **See col.2, lines 38-39;** discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 11:

Rix discloses a computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program, said method comprising the steps of:

generating a first cipher key from at least one first block of the encrypted computer program; **(col.2, lines 36-37 and col.3, lines 17-18)**

performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key; and **(col.2, lines 44-45)**

means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. **(col.1, lines 35-39 and col.2, lines 46-50)**

As per claim 12: **See col.2, lines 7-8;** discussing said at least one block is not encrypted.

As per claim 13: **See col.2, lines 36-37 and col.3, lines 17-18;** discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 14: **See col.2, lines 38-39;** discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 16:

Rix discusses data structure embodied on a computer-readable medium comprising:

a non-encrypted block; and **(col.2, lines 7-8)**

a plurality of encrypted blocks; **(col.1, line 31)**

wherein said plurality of encrypted blocks are encrypted with a cipher key generated from said non-encrypted block, and **(col.2, lines 32-36)**

wherein for each of said plurality of second blocks, a next block is encrypted with a cipher key which is generated from a current block. **(col.1, lines 35-39 and col.2, lines 36-37)**

As per claim 17:

Rix discloses a system for decrypting an encrypted computer program, comprising:

means for generating cipher keys for a plurality of blocks, and **(col.2, lines 32-33)**

means for performing a decryption of the plurality of blocks, **(col.2, lines 44-45)**

wherein for each of said plurality of second blocks, a cipher key is generated from a current block and a next block is decrypted said cipher key. **(col.1, lines 35-39 and col.2, lines 44-46)**

As per claim 18:

Rix discusses a system for decrypting an encrypted computer program, comprising a step of:

performing a decryption of the plurality of blocks, **(col.2, lines 44-45)**

wherein for each of said plurality of second blocks, a cipher key is generated from a current block and a next block is decrypted said cipher key. **(col.1, lines 35-39 and col.2, lines 44-46)**

As per claim 19:

Rix discusses a computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program, comprising a step of:

performing a decryption of the plurality of blocks, **(col.2, lines 44-45)**

wherein for each of said plurality of second blocks, a cipher key is generated from a current block and a next block is decrypted with said cipher key. **(col.1, lines 35-39 and col.2, lines 44-46)**

As per claim 20: **See col.3, lines 59-61;** discussing means for performing the second decryption of the plurality of second blocks executes the second decryption faster than said means for performing the first decryption of the plurality of second blocks.

As per claim 21: **See col.3, lines 59-61;** discussing means for performing the second decryption of the plurality of second blocks executes the second decryption faster than said means for performing the first decryption of the plurality of second blocks.

As per claim 22: **See col.3, lines 59-61;** discussing means for performing the second decryption of the plurality of second blocks executes the second decryption faster than said means for performing the first decryption of the plurality of second blocks.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 5, 10, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rix (US 6,766,024) in further view of Lotspiech, Et Al. (US 6,118,873).

As per claim 5:

Rix discloses a system for decrypting an encrypted computer program, comprising means for generating a first cipher key from at least one first block of the encrypted computer program **(col.2, lines 36-37 and col.3, lines 17-18),** means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key **(col.2, lines 44-45),** means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key **(col.1, lines 35-39 and col.2, lines 46-50).** However, Rix did not discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy

blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Rix with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech because by analyzing the program determines whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

As per claim 10:

Rix discloses a system for decrypting an encrypted computer program, comprising means for generating a first cipher key from at least one first block of the

encrypted computer program **(col.2, lines 36-37 and col.3, lines 17-18),** means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key **(col.2, lines 44-45),** means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key **(col.1, lines 35-39 and col.2, lines 46-50).** However, Rix did not discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Rix with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer

program is determined to be analyzed as taught by Lotspiech because by analyzing the program determines whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

As per claim 15:

Rix discloses a system for decrypting an encrypted computer program, comprising means for generating a first cipher key from at least one first block of the encrypted computer program **(col.2, lines 36-37 and col.3, lines 17-18),** means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key **(col.2, lines 44-45),** means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key **(col.1, lines 35-39 and col.2, lines 46-50).** However, Rix did not discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been

compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Rix with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech because by analyzing the program determines whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100